Nova Law Review

Volume 41, *Issue* 3 2017 *Article* 5

Keeping Internet Pirates At Bay: Ransomware Negotiation In The Healthcare Industry

Paul R. DeMuro*

*

Keeping Internet Pirates At Bay: Ransomware Negotiation In The Healthcare Industry

Paul R. DeMuro

Abstract

The law plays a significant role in all negotiations, regardless of the context

KEYWORDS: healthcare, pirates, ransomware

KEEPING INTERNET PIRATES AT BAY: RANSOMWARE NEGOTIATION IN THE HEALTHCARE INDUSTRY

PAUL R. DEMURO*

*. Paul R. DeMuro, PhD, JD, MBA, CPA is an Associate Professor, Department of Sociobehavioral and Administrative Pharmacy, College of Pharmacy, Nova Southeastern University, Fort Lauderdale, FL, and Of Counsel, Broad and Cassel, Fort Lauderdale, FL. He can be reached at pdemuro@nova.edu or pdemuro@broadandcassel.com. The author wishes to thank Henry Norwood, a student at Nova Southeastern University, Shepard Broad College of Law, for his extensive research and writing contribution to this article.

I. INTRODUCTION

The law plays a significant role in all negotiations, regardless of the context.[1] The law can determine the who, what, when, where, and why of all

1. *See* Lucas V.M. Bento, *Preserving Negotiation Whilst Promoting Global Order: Should We Bargain with Salt-Water Devils?*, 19 HARV. NEGOT. L. REV. 285, 297

negotiations.[2] Given the importance and power of law in the negotiation context, adopting clear legal principles tailored to negotiations in specific contexts will help willing and unwilling negotiators reach their desired outcomes.[3] Negotiation comes into play in a number of different areas, both legal and otherwise.[4]

One venue where the negotiation principles used in legal and non-legal areas coincide is the venue of ransom negotiations.[5] Like other negotiations, ransom negotiations feature adverse parties with competing interests struggling to promote their own ends.[6] With ransom negotiations, however, the stakes are often much higher than a standard negotiation and the party demanding the ransom payment has the opposing party at a distinct disadvantage.[7]

Ransom negotiations take place fairly often in the contexts of piracy and terrorism.[8] Several laws and a wealth of experience have shaped how negotiations in these contexts are able to progress.[9] Insights into negotiations in these contexts can be used to shape negotiations in favor of the party facing a ransom demand in a different ransom context—the context of cybercrime.[10] Cybercriminals continue to develop new inventive means of extorting valuable assets from computer users, including holding computer systems hostage.[11] Cybercriminals are employing viruses that lock a computer user out of their own system and demand payment in return for

---

(2014); Donald G. Gifford, *A Context-Based Theory of Strategy Selection in Legal Negotiation*, 46 OHIO ST. L.J. 41, 46 (1985); Alex J. Hurder, *The Lawyer's Dilemma: To Be or Not to Be a Problem-Solving Negotiator*, 14 CLINICAL L. REV. 253, 253–54 (2007).

2. *See* Bento, *supra* note 1, at 297; Gifford, *supra* note 1, at 46; Hurder, *supra* note 1, at 253–54.

3. *See* Bento, *supra* note 1, at 297; Gifford, *supra* note 1, at 46; Hurder, *supra* note 1, at 253–54.

4. *See* Bento, *supra* note 1, at 297; Gifford, *supra* note 1, at 46; Hurder, *supra* note 1, at 253–54.

5. *See 10-Minute Guide to Healthcare Ransomware Protection*, XTIUM, http://www.xtium.com/beta/wp-content/uploads/2016/07/Xtium_10-Minute-Guide-to-Ransomware-Protection.pdf (last visited May 2, 2017); Larry N. Zimmerman, *Ransomware — Your Data for Dollars*, J. KAN. B. ASS'N, Apr. 2015, at 16, 16.

6. *See* Bento, *supra* note 1, at 307–08.

7. *Id.* at 308, 311; *see also 10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

8. *See* Bento, *supra* note 1, at 299; Rivka Weill, *Exodus: Structuring Redemption of Captives*, 36 CARDOZO L. REV. 177, 180 (2014).

9. Bento, *supra* note 1, at 297–98; Weill, *supra* note 8, at 180–81.

10. GAVIN O'GORMAN & GEOFF MCDONALD, SYMANTEC, RANSOMWARE: A GROWING MENACE 2 (2012); Zimmerman, *supra* note 5, at 16.

11. O'GORMAN & MCDONALD, *supra* note 10, at 2; Dean F. Sittig & Hardeep Singh, *A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks*, 2016 APPLIED CLINICAL INFORMATICS 624, 625.

regained control of the system.[12] To make matters worse, these viruses are often capable of stealing private information from the captive computer as the virus locks down the system.[13] The healthcare industry, with its endless amount of electronic private patient information and high-demand environment, is especially at risk from the virus.[14]

This Article discusses the history, composition, and value of the ransomware virus, as well as its impact on the healthcare industry.[15] The Article then moves to a discussion of negotiation and legal theories applied to the contexts of piracy and terrorism.[16] After analyzing the existing legal framework of electronic private patient information in the healthcare industry, along with the best practices to avoid cyberattacks in the first place, negotiation theory is applied to the ransomware context to shed light on whether healthcare organizations should be permitted to engage in ransom negotiations with cybercriminals.[17]

II. THE BASICS OF RANSOMWARE

Ransomware, as its name suggests, is a type of computer malware designed to extort ransom payments from its targets.[18] Ransomware acts by infecting a computer, disabling the entire computer or disabling specific programs or functions of the computer, and presenting a message on the computer demanding a ransom payment in exchange for regaining the

12. COMPUT. CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE 2 (2016), http://www.justice.gov/criminal-ccips/file/872771/download [hereinafter CCIPS WHITE PAPER]; O'GORMAN & MCDONALD, *supra* note 10, at 2.

13. CCIPS WHITE PAPER, *supra* note 12, at 2.

14. Christiaan Beek, *Healthcare Organizations Must Consider the Financial Impact of Ransomware Attacks*, MCAFEE (Apr. 21, 2016), http://securingtomorrow.mcafee.com/executive-perspectives/healthcare-organizations-must-consider-financial-impact-ransomware-attacks/; Mark Hagland, *Special Report on Data Security: With the Ransomware Crisis, the Landscape of Data Security Is Shifting*, HEALTHCARE INFORMATICS (May 26, 2016), http://www.healthcare-informatics.com/article/special-report-data-security-ransomware-crisis-landscape-data-security-shifting.

15. *See infra* Part II.

16. *See infra* Parts II, III.

17. *See infra* Section IV.

18. CCIPS WHITE PAPER, *supra* note 12, at 2; Alexandre Gazet, *Comparative Analysis of Various Ransomware Virii*, 6 J. COMPUTER VIROLOGY & HACKING TECH. 77, 77 (2010).

computer's functionality.[19] Ransomware has taken on many different forms and has evolved since its birth many years ago.[20]

A. *The History of Ransomware*

The original ransomware would infect a computer, encrypt certain files in the computer so that the user could not open them without an decryption key, and demand a ransom payment in exchange for the decryption key.[21] The modern day ransomware is capable of locking an infected computer's screen, rendering the computer useless to the user.[22] The virus will then display a message demanding payment in exchange for regained access to the computer.[23] This modern form of ransomware is believed to have originated near Russia.[24] Instead of simply demanding a ransom payment and disclosing the criminal nature of the screen lock, some early forms of ransomware would instead display a message on the infected computer purporting to be from Microsoft and claiming that in order to activate the computer, the user must send a text message to a phone number which would charge the user a premium charge for the text.[25] The user would thus be sending what he or she thought was a simple activation text to Microsoft, but in reality his or her computer had been infected with ransomware and the premium charge from the text message was being collected by the hacker.[26] Another early variant of the virus did not bother with concealing the criminal nature of the ransom and instead of posing as a representative of Microsoft, the hacker would simply display a pornographic image on the user's screen and lock the screen with the image on display.[27] The hacker would then send a message demanding payment through a similar premium charge phone call or text message as the Microsoft variant, in exchange for removal of the pornographic image and regained computer function.[28] This version of ransomware was successful by shaming the

19. O'GORMAN & MCDONALD, *supra* note 10, at 2; LYNNE DUNBRACK, IDC HEALTH INSIGHTS, PROVIDING OUTSIDE-IN AND INSIDE-OUT PROTECTION AGAINST RANSOMWARE AND OTHER INTENSIFYING CYBERTHREATS 2 (2016).

20. *See* O'GORMAN & MCDONALD, *supra* note 10, at 2.

21. *Id.* at 3; *see also* CCIPS WHITE PAPER, *supra* note 12, at 2.

22. O'GORMAN & MCDONALD, *supra* note 10, at 2; CCIPS WHITE PAPER, *supra* note 12, at 6.

23. O'GORMAN & MCDONALD, *supra* note 10, at 2; CCIPS WHITE PAPER, *supra* note 12, at 2.

24. O'GORMAN & MCDONALD, *supra* note 10, at 3.

25. *Id.* at 4.

26. *Id.*

27. *Id.*

28. *Id.*

computer's user into paying the ransom and this version lasted for quite some time.[29]

Starting around 2011, a new ransomware variant was introduced.[30] The virus is similar to its predecessor in that the virus still locks the user's computer screen or locks the user out of specific computer files.[31] The major difference is in the content of the ransom message displayed on the computer user's screen.[32] The new displayed messages claim to be from a government agency, such as the Federal Bureau of Investigation ("FBI"), or from a local law enforcement agency.[33] The fake message would inform the user that his or her computer had been locked because the user had committed a crime and the only way to regain access would be to pay a fine for the crime.[34] Interestingly, some forms of the virus use accessible location services in order to determine where the infected computer is located geographically.[35] Determining where the computer is located allows the hacker to tailor the ransom message to appear more legitimate, such as by ensuring the message is written in the predominant language where the computer is located and by displaying law enforcement images portraying the agencies existing in that country.[36] This new ransomware also abandoned the premium charge text and phone method of collecting its ransoms.[37] Modern ransomware hackers now take advantage of online pre-payment methods, which act similarly to online pre-paid visas.[38] The computer user loads funds into an online account, which the hacker has access to using his or her own credit card.[39] The hacker then retrieves the funds and decides whether to unlock the victim's computer or dishonor their agreement.[40]

B. *How Does Ransomware Infect Computers?*

Of course, in order to ever succeed in their goal of extorting a ransom from their victims, hackers must first infect computers with the

29. O'GORMAN & MCDONALD, *supra* note 10, at 4.
30. *Id.*
31. *Id.*; Gazet, *supra* note 18, at 77; Zimmerman, *supra* note 5, at 16.
32. *See* O'GORMAN & MCDONALD, *supra* note 10, at 4.
33. *Id.* at 2.
34. *Id.* at 4; *see also* Gazet, *supra* note 18, at 77; Zimmerman, *supra* note 5, at 16.
35. O'GORMAN & MCDONALD, *supra* note 10, at 5.
36. *Id.*
37. *Id.* at 4–5.
38. *Id.* at 5.
39. *Id.*
40. O'GORMAN & MCDONALD, *supra* note 10, at 6; *see also 10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

ransomware virus.[41] There are many different techniques used by hackers to infect computers with the ransomware virus.[42] One of the most common methods used is referred to as a *drive-by download*.[43] A drive-by download occurs when the hacker has already gone through the process of hacking into a website.[44] The hacker then inserts hidden malware onto the website.[45] An unsuspecting person visiting the website will automatically be redirected to a second website operated by the hacker, which installs the ransomware onto the person's computer.[46] In order to hack into a website in the first place, the website must have some type of vulnerability that the hacker can exploit.[47]

To avoid the hassle of exploiting an already existing weakness in a website, some hackers legitimately buy advertising space on a website.[48] The advertisement may purport to be promoting anything, but once the user clicks on the advertisement, the user is directed to the hacker's website containing the ransomware virus.[49]

A different tactic used by hackers is referred to as *spear phishing*.[50] Spear phishing is a hacking technique where the hacker sends a false email to an employee of a company.[51] The email may claim to be from the employee's coworker or supervisor and may instruct the employee to follow a series of tasks, which would actually result in the employee infecting his or her system with a virus, such as ransomware.[52]

Other means of infecting computers with the ransomware virus include piggybacking the virus onto a different form of malware already infecting a computer, or by sending out emails containing spam along with the virus.[53] Ransomware will often be paired with another form of malware designed specifically to steal data and other information located on the infected computer.[54] Thus, while the ransomware virus locks the computer

41. O'GORMAN & MCDONALD, *supra* note 10, at 2; Hagland, *supra* note 14.
42. O'GORMAN & MCDONALD, *supra* note 10, at 2.
43. *Id.* at 4; *see also* DUNBRACK, *supra* note 19, at 1.
44. O'GORMAN & MCDONALD, *supra* note 10, at 4.
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. O'GORMAN & MCDONALD, *supra* note 10, at 4.
50. DUNBRACK, *supra* note 19, at 1–2; Hagland, *supra* note 14; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
51. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; *see also* DUNBRACK, *supra* note 19, at 2.
52. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; *see also* DUNBRACK, *supra* note 19, at 2.
53. DUNBRACK, *supra* note 19, at 10; *see also* O'GORMAN & MCDONALD, *supra* note 10, at 4.
54. CCIPS WHITE PAPER, *supra* note 12, at 8.

and demands ransom from the victims, the additional malware is stealing data from the hostage computer.[55]

While the version of ransomware which requires a computer user to click on a certain advertisement or email is still commonly used, newer versions of the virus are being developed that rely on vulnerabilities in an organization's web server.[56] If a healthcare organization's web server is unprotected or *unpatched*, hackers are able to exploit this weakness and infiltrate the organization's online network.[57] Once inside the network, the virus is able to move from the initial hacked computer to other computers using the same network, collect login data and credentials from employee staff, steal private stored data, and infect multiple systems with the ransomware virus.[58]

C. *Ransomware and the Black-Market Economy*

The earning prospects for cybercriminals using the ransomware virus vary by country and by virus.[59] In one study, a variant of the virus was discovered to have infected 5700 computers in approximately one day.[60] Of this number, 168 users appear to have tried to free their computers by entering a pin number, which is given to the user by the hacker after the user pays the demanded ransom.[61] The study demonstrated that the number of users who potentially paid the ransom was approximately 2.9% of those infected, the average amount demanded was $200, and that this would result in the hackers extorting $33,600 in ransom payments in a single month using this variant of the ransomware virus.[62] Expanding this finding to an entire year, the researchers concluded that an estimated $394,400 could be transferred in ransom in an entire year with this virus if only 2.9% of the yearly targets pay.[63] As of the beginning of 2016, over 4000 cyberattacks using the ransomware virus have occurred every single day on average.[64] This number marks an increase of 300% when compared to the number of attacks that occurred in 2015.[65] While these numbers alone are sufficiently

55. *Id.*
56. *See* DUNBRACK, *supra* note 19, at 2; O'GORMAN & MCDONALD, *supra* note 10, at 4.
57. DUNBRACK, *supra* note 19, at 2.
58. *Id.*
59. O'GORMAN & MCDONALD, *supra* note 10, at 6.
60. *Id.*
61. *Id.*
62. *Id.*
63. *Id.*
64. CCIPS WHITE PAPER, *supra* note 12, at 2.
65. *Id.*

significant to demonstrate the growing threat of ransomware, they may represent only a fraction of the total sums extorted from organizations, as many organizations do not report being attacked by ransomware hackers, nor do they report paying the hacker a ransom.[66]

The ransomware virus is being used by hackers moderately to aggressively target computers in the United States.[67] Just as the virus itself has evolved over time, so has its targets.[68]

D. *The Threat of Ransomware in the Healthcare Setting*

Healthcare organizations are appealing targets to hackers.[69] In 2015, healthcare organizations were targeted by cybercriminals more than most other industries.[70] Some research suggests that on average, healthcare organizations experience a cyberattack almost every single month.[71] The same research also suggests that nearly half of the healthcare organizations involved in the study had experienced a cyberattack within the past twelve months in which private patient information was at risk.[72]

---

66. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5. There are a number of reasons why an organization may choose not to report an attack. CCIPS WHITE PAPER, *supra* note 12, at 5. If word gets out that the organization was successfully attacked or, even worse, that the organization paid a hacker's ransom demands, other cybercriminals may be encouraged to attack the organization upon seeing its willingness to pay or upon discovering its cyber-vulnerability. *Id.* The organization that pays a ransomware hacker may also be met with a negative reputation if word of the payment gets out because the organization has indirectly financed criminal activity. *Id.*

67. O'GORMAN & MCDONALD, *supra* note 10, at 9; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5. In May of 2017, a series of ransomware attacks worldwide resulted in hundreds of thousands of computer systems being infected from over one-hundred countries. Ross Koppel & Harold Thimbleby, *Lessons from the 100 Nation Ransomware Attack*, THE HEALTH CARE BLOG (May 14, 2017), http://thehealthcareblog.com/blog/2017/05/14/lessons-from-the-100-nation-ransomware-attack/. The variant of the ransomware virus employed in these attacks has been labeled "WannaCry" and is believed to have been developed based on vulnerabilities in Microsoft operating systems, which were originally discovered by the U.S. National Security Agency. *Id.*; David Goldman, *Global Cyberattack: A Super-Simple Explanation of What's Going on*, CNN (May 15, 2017), http://money.cnn.com/2017/05/14/technology/global-cyberattack-explanation/index.html.

68. Hagland, *supra* note 14.

69. *Id.*

70. *Id.*

71. PONEMON INST., THE STATE OF CYBERSECURITY IN HEALTHCARE ORGANIZATIONS IN 2016 (2016), http://cdn1.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf.

72. *Id.*

The ransomware virus has been very effective at infecting healthcare organizations.[73] Between 2005 and 2014, $57.6 million in ransom payments were made by healthcare organizations to ransomware hackers.[74] During these years, ransom payments to hackers ranged from $200 to $10,000.[75] However, in the year of 2015 alone, approximately $24 million in ransom payments were made by healthcare organizations to ransomware hackers.[76] On February 12th, the Hollywood Presbyterian Medical Center in Hollywood, California fell prey to a ransomware attack.[77] A doctor of the medical center claimed that the medical center's system "was being held for ransom."[78] Later reports indicated that the health center had lost control of its electronic health record system for longer than a week and that those responsible demanded over $3 million in order to bring the medical center's system back online.[79] The CEO for the hospital later revealed that the medical center had paid approximately $17,000 to the hackers and the hackers had honored their word and restored the medical center's access to their system.[80] A March 28th incident revealed that integrated systems storing health data were also at risk when a Columbia-based integrated healthcare system was targeted by a ransomware virus.[81] The system stored information for ten hospitals and the information systems reportedly took several weeks to restore while the hospitals attempted to function and care for patients as best as possible.[82] A single attack on a Maryland-based hospital led to an $18,500 ransom payment.[83]

Healthcare organizations are an appealing target to data hackers.[84] Patients' electronic health records are worth far more than a victim's credit or debit card number.[85] In fact, data indicates that electronic health records

73. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
74. *Id.*
75. *Id.*
76. *Id.*
77. Hagland, *supra* note 14.
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. Hagland, *supra* note 14.
83. DUNBRACK, *supra* note 19, at 2.
84. *See 10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; Beek, *supra* note 14; William Maruca, *Hacked Health Records Prized for their Black Market Value*, FOX ROTHSCHILD LLP: HIPPA, HITECH & HIT (Mar. 16, 2015), http://hipaahealthlaw.foxrothschild.com/2015/03/articles/articles/hacked-health-records-prized-for-their-black-market-value/.
85. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; Kevin Lonergan, *Why the Healthcare Industry Badly Needs a Cyber Security Health Check*,

may be worth ten times more to data hackers than a credit or debit card number.[86] In 2015, there was a larger volume of U.S. based ransomware attacks than previously, specifically focusing on the healthcare industry.[87] Healthcare organizations may be so appealing to hackers because every minute could literally be a matter of life and death, and every minute the organization does not have full access to its electronic information, each patient is at risk.[88]

As noted above, electronic health records are extremely valuable to cyber hackers.[89] Healthcare organizations are using and creating more electronic healthcare data than ever before.[90] Electronic healthcare data allows healthcare providers different advantages to providing patients with quality care; however, with more data being stored in an online format, hackers have more targets and far more incentive to target the healthcare industry.[91] Healthcare organizations are storing "valuable financial, insurance, and demographic data" which can be used, or sold to be used, to commit identity theft.[92]

As an additional threat, hospital employees and medical staff are now using their personal or organization-provided mobile devices in order to access private patient health records stored on the organization's servers.[93] Alerts are sent to the mobile devices of healthcare staff to keep them informed of patients' vital statistics.[94] *Medical imaging machines* are connected to healthcare servers using the Internet.[95] New technologies are being developed that allow constant health monitoring of patients by healthcare professionals, such as smart glasses.[96] This constant stream of private health information is recorded and digitally sent to the healthcare organization's servers where it becomes accessible to the monitoring healthcare professional.[97] Older technology, such as copy machines, are also

---

INFO. AGE (Aug. 25, 2015), http://www.information-age.com/why-healthcare-industry-badly-needs-cyber-security-health-check-123460052/; Maruca, *supra* note 84.

86. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; Lonergan, *supra* note 85; Maruca, *supra* note 84.

87. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

88. *See* DUNBRACK, *supra* note 19, at 1–3.

89. *See 10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; Lonergan, *supra* note 85; Maruca, *supra* note 84.

90. DUNBRACK, *supra* note 19, at 2–3.

91. *Id.*

92. *Id.* at 2.

93. *Id.* at 3.

94. *Id.*

95. DUNBRACK, *supra* note 19, at 3.

96. *Id.*

97. *See id.*

connected to the organization's servers.[98] Unfortunately, these technologies are very vulnerable to cyberattacks.[99] It seems that as the technology itself boldly strides forward, the efforts to secure and protect the information being sent by the technologies are left behind.[100]

E. *Using a Negotiation Theory Approach to Solving the Ransomware Problem*

Intelligent negotiation can aid in dispute-resolution without having to deal with lengthy and costly conflicts.[101] Negotiators employing what is referred to as the *problem-solving approach* to negotiations appreciate the costs and benefits of each side of the negotiation and seek to reach a resolution beneficial to both sides.[102] The problem-solving negotiator seeks creative solutions to disputes that will satisfy, at least in part, the goals of each party.[103] Negotiation theory is an ideal framework from which to analyze negotiations with ransomware hackers, as it takes into account the costs and benefits of ransom negotiations, as well as considering other external factors, such as the legal landscape surrounding the negotiation and the human costs of ransom negotiations, which can aid negotiators dealing

98. *Id.*

99. *Id.* at 4. Hackers are already using these new technologies to breach healthcare organization's networks. *See* DUNBRACK, *supra* note 19, at 4. Connected technologies including "insulin pumps, heart monitors, and picture archiving and communication systems" have already been hacked in order to gain access to the connected healthcare organization's network. *Id.*

100. *Id.* Ransomware hackers are able to use these new technologies as back doors to gain access to a healthcare network. *Id.* The hacker no longer needs to find vulnerabilities in the organization's network itself, but instead hackers can breach the more vulnerable healthcare technologies that are connected and transmitting information to the network. *Id.* This type of back door hacking is known as *medjacking*. DUNBRACK, *supra* note 19, at 4. After breaching the single, connected device, the hacker can use the virus to infiltrate the organization's network and move from system to system on the network, infecting devices, and stealing information. *See id.* Once infected, cybercriminals could "take . . . control of the [specific] device" itself, but this is uncommon, and hackers normally use these devices as a means of gaining access to the more lucrative prize of the connected organization's network. *Id.* Healthcare organizations are woefully unprepared for this type of threat as most organizations have not integrated these new technologies into their existing security framework. *See id.*

101. Hurder, *supra* note 1, at 254.

102. *Id.* at 254, 273.

103. CHARLES B. CRAVER, EFFECTIVE LEGAL NEGOTIATION AND SETTLEMENT 11–12 (7th ed. 2012); *see also* SPENCER PUNNETT, REPRESENTING CLIENTS IN MEDIATION: A GUIDE TO OPTIMAL RESULTS BASED ON INSIGHTS FROM COUNSEL, MEDIATORS, AND PROGRAM ADMINISTRATORS 412 (2013); Gifford, *supra* note 1, at 46.

with ransomware hackers and other criminal hostage-takers to achieve optimal results.[104]

III. NEGOTIATING WITH PIRATES

Piracy poses a major threat across the globe to human life, the global economy, and the environment.[105] Pirates who engage in hostage-taking for ransom payments put ransom negotiators in the position to save lives, while trying not to financially benefit the pirates.[106] Effective negotiation can reduce these costs and creative legal strategies can reduce the incidence of piracy worldwide.[107]

A. *Piracy in the Modern Age*

Piracy has become an increasing problem over the past decade.[108] In 2008, pirates committed or attempted roughly 293 attacks.[109] In 2012, the number of attacks increased to roughly 300.[110] Pirates long ago realized that simply to pillage and plunder a seized vessel was a wasted opportunity when the vessel's crew could be ransomed off for far more lucrative bounties.[111] In fact, the ransoming of crewmembers has largely become the primary motivation for modern-day pirates seizing maritime vessels.[112] Between 2008 and early 2014, ransom payments exceeding $300 million had been paid to pirates.[113] In 2011, more than 1200 people were held for ransom by pirates.[114] Of this number, 35 of the hostages and 111 pirates died during the process.[115] Further, many piracy attacks never go reported at all, as ship owners try to keep the attacks quiet in order to avoid increased insurance

104. *See* CRAVER, *supra* note 103, at 11–12; PUNNETT, *supra* note 103, at 412; Bento, *supra* note 1, at 305; Gifford, *supra* note 1, at 46.

105. Daniel Pines, *Maritime Piracy: Changes in U.S. Law Needed to Combat this Critical National Security Concern*, 36 SEATTLE U. L. REV. 69, 71 (2012).

106. *See* Bento, *supra* note 1, at 313–14, 321–22.

107. *See id.* at 287–88, 292, 326; Hurder, *supra* note 1, at 254.

108. *See* Bento, *supra* note 1, at 294.

109. ICC Int'l Maritime Bureau [IMB], *Privacy and Armed Robbery Against Ships: Report for the Period 1 January–31 December 2012*, at 5–6 (Jan. 2013).

110. *Id.*

111. Bento, *supra* note 1, at 287, 304.

112. *Id.* at 287.

113. Paul Redfern, *Over $300m Paid in Ransom to Pirates Since 2008*, THE E. AFR. (Feb. 9, 2013, 8:40 PM), http://www.theeastafrican.co.ke/news/Over-USD300m-paid-in-ransom-to-pirates-since-2008/2558-1689648-jxsa4h/index.html.

114. ICC IMB, *supra* note 109, at 24.

115. *Id.*

premiums.[116] While the costs of human life and ransom payments may be the most prominent costs of piracy, there are also secondary costs involved in piracy situations, such as the costs to deliver the ransom, to repair damaged vessels, to replace stolen cargo, to pay for legal services, etc.[117] The pirates' course is simple: Seize the vessel while ensuring its continued navigability and seize the crew in order to maximize the pirates' expected return for their efforts.[118] The negotiation phase begins here and the stakes could not be higher: The lives of the sailors.[119]

B. *The Piracy Ransom Negotiation Context*

Recent history is replete with graphic examples of negotiations with pirates gone bad for many of the same reasons negotiations in the business or legal setting turn sour—miscommunication, refusal to cooperate, delayed payments, an aggressive negotiation style, technical difficulties, etc.[120] In 2011, Somali pirates seized and killed four American sailors when negotiations fell apart between the pirates and the U.S. Navy.[121] The next year, Somali pirates killed a sailor over the delay of a ransom payment.[122]

Grisly illustrations of negotiations with pirates gone south tend to cloud the public's perception of how pirates view these transactions: It is only business.[123] From a pirate's perspective, ransoming sailors is nothing more than a matter of financial gain.[124] This is one of the major details separating the pirate from the terrorist.[125] Although ransom situations may result in harm or death to the hostage crew, such situations may also conclude with the successful release of the hostages after the ransom is paid.[126] In 2012, pirates attacked a Greek vessel and held its crew for

116. Bento, *supra* note 1, at 293.
117. *Id.* at 291.
118. *See* Yvonne M. Dutton & Jon Bellish, *Refusing to Negotiate: Analyzing the Legality and Practicality of a Piracy Ransom Ban*, 47 CORNELL INT'L L.J. 299, 301, 305–06 (2014).
119. *See* Bento, *supra* note 1, at 291.
120. *See id.* at 287–88.
121. *Id.*
122. *Id.* at 288; *see also* Dutton & Bellish, *supra* note 118, at 301.
123. *See* Pines, *supra* note 105, at 73–74, 78.
124. *See id.* at 78.
125. *See* Bento, *supra* note 1, at 303–04.
126. *See* Barry Hart Dubner & Kimberly Chavers, *The Dilemma of Piratical Ransoms: Should They Be Paid or Not? On the Human Rights of Kidnapped Seamen and Their Families*, 18 BARRY L. REV. 297, 300 (2013); Thaine Lennox-Gentle, *Piracy, Sea Robbery, and Terrorism: Enforcing Laws to Deter Ransom Payments and Hijacking*, 37 TRANSP. L.J. 199, 200 (2010). Between January and December of 2012, approximately 585

ransom.[127] The pirates successfully ransomed the crew for $5 million and accordingly spared the crew.[128] If pirates never intend to make good on their ransom deals, they would eventually cease to exist because ransoms would no longer be paid.[129]

The ransoms negotiated by pirates provide a means of financial support to both the pirate and to the local economy of the pirate's community.[130] The correlation between dismal local economic conditions and piracy provides insight into a pirate's motivations.[131] While the pirates' actions are certainly deplorable, ignoring their motivations is a critical mistake for the negotiator on the other side of the table.[132]

Attorney Lucas V.M. Bento distinguishes between three different interests at play in ransom negotiations with pirates.[133] Non-pecuniary interests are those involving "the well-being of hostages during captivity, their safe release and post-incident care."[134] Pecuniary interests are those involved in recovering the vessel and its cargo.[135] Lastly, hybrid interests are a combination of the first two interests.[136] Bento explains that, although the majority of ransom negotiations involve hybrid interests, non-pecuniary interests tend to be more concerning.[137]

Beyond the financial and non-financial interests at stake in pirate ransom negotiations, understanding the nature and complexity of pirate organizations is vital to reaching desired outcomes.[138] Pirate organizations can vary in their sophistication just like other criminal syndicates.[139] The pirates physically present and boarding their target vessels may not have the clout in a negotiation to make decisions on behalf of the pirate

---

sailors were held as hostages by pirates. Dubner & Chavers, *supra*, at 300. Of this total number, the pirates killed six of the sailors, leaving the remaining sailors alive. *Id.*

127. Bento, *supra* note 1, at 295.

128. *Id.*

129. Dutton & Bellish, *supra* note 118, at 301.

130. *See id.* at 305–06.

131. *See* Dubner & Chavers, *supra* note 126, at 298–99; Lennox-Gentle, *supra* note 126, at 205; Pines, *supra* note 105, at 77–78.

132. *See* Gifford, *supra* note 1, at 60–62; Lennox-Gentle, *supra* note 126, at 205; Jennifer W. Reynolds, *Breaking BATNAS: Negotiation Lessons from Walter White*, 45 N.M. L. REV. 611, 612 (2015).

133. Bento, *supra* note 1, at 291. Lucas V.M. Bento is an attorney based in New York specializing in international disputes and arbitration. *Id.* at 285 n.*.

134. *Id.* at 291.

135. *Id.*

136. *Id.*

137. Bento, *supra* note 1, at 291.

138. *See* Lennox-Gentle, *supra* note 126, at 205.

139. Dutton & Bellish, *supra* note 118, at 306; Lennox-Gentle, *supra* note 126, at 205–06.

organization.[140] For the negotiator opposing the pirates, it is paramount to discover whether the pirates involved in the discussion have the authority to make flexible decisions or whether they are strictly following a preconceived plan with no option to deviate.[141] Shedding light on all of the inner workings of a pirate organization is often impossible, but by putting in the effort to learn as much about the organization as possible, the opposing negotiator can increase the chances of arriving at a desired outcome.[142]

C. *Arguments Against Paying Ransoms to Pirates*

International state actors differ in their approaches to addressing the problem of negotiating with and paying ransoms to pirates.[143] Many nations, including the United States, France, Britain, Columbia, and Italy, as a matter of policy, oppose paying ransoms to pirates to free hostages, however these countries do not make the payment of pirate ransoms illegal.[144] Somalia has illegalized the payment of ransoms to pirates.[145] The opponents of paying ransoms to pirates contend that giving in to ransom demands only emboldens the pirates and encourages them to commit similar acts in the future because the pirates know their demands will be met.[146] Further, opponents believe that paying ransoms indirectly funds the enterprise of piracy, thus giving the same pirates the means to conduct additional operations.[147] An argument against paying a pirate's ransom demands, often employed by the United States, is that piracy is commonly intertwined with other international crimes, such as terrorism.[148] While international terrorism is a separate international crime from piracy, paying a ransom demand in response to one crime may end up resulting in the other.[149]

In 2010, former President of the United States, Barack Obama, issued an executive order banning any financial transactions with certain

140. *See* Dutton & Bellish, *supra* note 118, at 305–06.

141. *See id.* at 301, 306; Pines, *supra* note 105, at 78.

142. *See* Lennox-Gentle, *supra* note 126, at 205.

143. *See* Bento, *supra* note 1, at 288–89; Dubner & Chavers, *supra* note 126, at 317–22; Lennox-Gentle, *supra* note 126, at 206–07.

144. Bento, *supra* note 1, at 288–89; Dubner & Chavers, *supra* note 126, at 320–22; Lennox-Gentle, *supra* note 126, at 206.

145. *Somalia: Six Jailed for 'Pirate Ransom' Cash*, BBC (June 20, 2011), http://www.bbc.co.uk/news/world-africa-13826050; *see also* Bento, *supra* note 1, at 288–89.

146. Bento, *supra* note 1, at 288–89; Dutton & Bellish, *supra* note 118, at 309–10.

147. Bento, *supra* note 1, at 289; Dutton & Bellish, *supra* note 118, at 309–310.

148. Bento, *supra* note 1, at 290; Lennox-Gentle, *supra* note 126, at 215.

149. Bento, *supra* note 1, at 290; Lennox-Gentle, *supra* note 126, at 214–15.

Somali organizations, some of which had ties to pirate gangs.[150] The United Kingdom ("U.K.") similarly criminalizes ransom payments made to pirate gangs with sufficient links to terrorist organizations.[151] Thus, although very few state actors go as far as to illegalize ransom payments to pirates, some states ban these payments if there is a threat that the funds may end up in terrorist hands.[152] The economic success of piracy has led to a *pirate stock exchange*, through which individual or corporate investors are actually investing in and receiving a cut of ransom payments given to pirates.[153] Paying ransoms to pirates may encourage the growth of and continued investments to the industry of piracy globally.[154]

D. *Arguments in Favor of Paying Ransoms to Pirates*

The maritime industry, however, has expressed concern that an outright ban on ransom payments would put sailors' lives at risk and significantly hamper the industry as a whole.[155] After all, what sailor would be interested in traversing pirate-infested waters with the knowledge that, if taken for ransom, nobody would be answering the call?[156] Proponents of paying ransoms to spare the lives of hostages also note that, even if ransom payments are made illegal, pirates may simply amplify their violence toward hostages in order to compel the sailors' family members—as well as ship owners—to make the illegal ransom payments.[157]

E. *Negotiation Solutions to the Ransom Problem: The Piracy Context*

Many scholars argue against an absolute ban on negotiations with pirates.[158] The varying interests of all parties involved should be weighed in

150. Bento, *supra* note 1, at 290.

151. CHATHAM HOUSE, PIRACY AND LEGAL ISSUES: RECONCILING PUBLIC AND PRIVATE INTERESTS 15 (2009).

152. *See* Dutton & Bellish, *supra* note 118, at 320, 322; Lennox-Gentle, *supra* note 126, at 214–15.

153. Avi Jorisch, *Today's Pirates Have Their Own Stock Exchange*, WALL STREET J. (June 16, 2011), http://www.wsj.com/articles/SB10001424052702304520804576341223910765818.

154. Dutton & Bellish, *supra* note 118, at 306–07.

155. *Id.* at 313–14; Dubner & Chavers, *supra* note 126, at 319.

156. *See* Dubner & Chavers, *supra* note 126, at 319.

157. *See* ADJOA ANYIMADU, CHATHAM HOUSE, COORDINATING AN INTERNATIONAL APPROACH TO THE PAYMENT OF RANSOMS: POLICY OPTIONS FOR REDUCING RANSOM PAYMENTS 8 (2012); Dubner & Chavers, *supra* note 126, at 319.

158. Bento, *supra* note 1, at 326, 330; Dubner & Chavers, *supra* note 126, at 327.

order to assess the potential payoffs of each approach to the problem.[159] The options available to governments and private parties or corporations facing ransom demands are either to pay the ransom or not to pay the ransom.[160] The options available to pirates demanding ransom are either to release the hostages or not to release the hostages.[161] Of these potential options, there is only one possible solution that benefits both parties: Where the government or private party pays the ransom and the pirates release the hostages.[162] If the private party chooses not to pay the ransom and, by some miracle, the pirates choose to release the hostages unharmed, the private party will have achieved its goal in the negotiation, whereas the pirates' goal will have been thwarted.[163] If the private party pays the ransom, but the pirates do not release the hostages, or if the pirates kill the hostages, then the private party will have been thwarted, and the pirates will have achieved their goal.[164] Lastly, if the private party chooses not to pay the ransom and the pirates choose not to release the crew—a scenario seen often—then neither party will have achieved their goals.[165]

While this framework provides a view of the competing interest of the parties, it is insufficient on its own to shed light on an appropriate policy regarding paying ransoms to pirates.[166] First, each option cannot be given equal weight, since the outcome in which the private party does not pay the ransom and the pirates release the hostages is unlikely; the outcome in which the private party pays the ransom and the pirates do not release the hostages is, at least, somewhat likely; and the situation where the private party pays the ransom and the pirates release the hostages can hardly be said to be an absolute win for the private party.[167] The private party is already at a loss for having to negotiate with pirates to begin with, and thus, the parties are on unequal footing going into the negotiation.[168] A key argument against paying ransoms is to prevent the funding of future criminal activity, a

159. *See* Bento, *supra* note 1, at 326, 330.
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. Bento, *supra* note 1, at 326, 330.
165. *Id.* In 2010, seven crewmembers were held hostage by pirates aboard the vessel, the Iceberg 1, for 800 days while the pirates' demands for ransom went ignored. *See Why David Cameron Will Not Stop Somali Pirates Getting Their Pieces of Eight*, COLINFREEMANSITE (Sept. 6, 2012), http://www.colinfreemansite.wordpress.com/2012/09/06/why-david-cameron-will-not-stop-somali-pirates-getting-their-pieces-of-eight/. During this time, one of the crewmembers committed suicide. *Id.* The situation was resolved by military intervention. *Id.*
166. *See* Bento, *supra* note 1, at 326, 330.
167. *See id.*
168. *See id.*

response to which this analysis does not provide.[169] However, completely banning private parties from paying ransoms to pirates could likely result in loss of life and remove that important option from the private party negotiator.[170]

This struggle between two options, which many perceive as unacceptable, has led scholars to propose more creative solutions to the problem.[171] A starting proposal argues that while private parties should be permitted to negotiate with and pay ransoms to pirates, state actors, such as the United States and the U.K., should have an absolute non-negotiation policy.[172] That approach ensures state actors take a stance against the actions of pirates and, ideally, will work toward reducing and eliminating the source of the problem, piracy itself.[173] Another solution is to permit private parties to pay ransoms to pirates, but to tax the ransom payments.[174] The benefits of this solution are twofold: First, additional funds are raised which can be applied toward combatting piracy; and second, those in charge of the ships at risk will be incentivized to take extra care to prevent these situations from occurring and protecting their vessels as best as possible.[175] The detriment of this solution is that victims of piracy are essentially being taxed for paying to spare the lives of their crew.[176] A further solution proposes holding ship-owners liable to their crew for failing to properly safeguard them from pirates.[177] The United States already permits sailors to sue ship-owners for negligence in situations involving pirate raids and for sending sailors into areas the owners know are plagued by pirate attacks.[178] Another solution would be to require ship-owners to employ guards on voyages through

169. *See id.* at 327; Dutton & Bellish, *supra* note 118, at 313.

170. Dutton & Bellish, *supra* note 118, at 314.

171. Bento, *supra* note 1, at 330–33; Dutton & Bellish, *supra* note 118, at 324–27.

172. *See* Bento, *supra* note 1, at 330 n.278.

173. *Id.*

174. *Id.* at 331.

175. *Id.* This solution also provides a silver lining to those opponents of paying any type of ransom to criminal pirates, in that the pirates who hold sailors for ransom are indirectly supporting the efforts to end piracy. *Id.* at 332. When private parties pay ransoms to pirates—in a sense rewarding pirates for their criminal activity—these ransom payments will then be taxed, and the proceeds will contribute to government efforts aimed at stopping piracy. Bento, *supra* note 1, at 332.

176. *Id.* at 331. An additional downside of this approach is that private companies paying ransoms for the release of their crew will be faced with an incentive not to report the incident at all in order to avoid being taxed on the ransom payment. *Id.* at 332.

177. *Id.* at 331.

178. *Id.* at 331–32.

pirate-infested waters.[179] In 2009, the U.S. Coast Guard required ships traveling in dangerous areas near Africa to employ guards.[180]

Negotiating with pirates need not feature an all-or-nothing outlook, in which a party either closes off from negotiations or where a party pays every ransom.[181] A cost-benefit analysis should be conducted during every negotiation to ensure that the negotiator is able to maximize its benefits, minimize its losses, and weigh context-based factors accordingly.[182] The ransom negotiator must also consider governmental efforts to curb piracy, such as taxes on ransom payments and ship-owner liability.[183]

IV. NEGOTIATING WITH TERRORISTS

Terrorists frequently participate in kidnapping to bankroll their other terrorist activities.[184] Ransoming off victims of terrorist kidnappings is highly lucrative and reports in recent years indicate that terrorists are receiving higher ransom rewards than in the past.[185] Newer terrorist organizations, such as the Islamic State of Iraq and the Levant ("ISIL"), have used the tactic with great success and have shed light on the different approaches taken by various countries in dealing with ransom negotiations with terrorists.[186]

---

179. *See* Bento, *supra* note 1, at 331.

180. *Id.*

181. *See id.* at 326; Gifford, *supra* note 1, at 60–62; Reynolds, *supra* note 132, at 612.

182. Bento, *supra* note 1, at 326, 330; Gifford, *supra* note 1, at 60–62; Reynolds, *supra* note 132, at 612.

183. Bento, *supra* note 1, at 331; *see also* Dutton & Bellish, *supra* note 118, at 325–27.

184. Sima Kazmir, *The Law, Policy, and Practice of Kidnapping for Ransom in a Terrorism Context*, 48 N.Y.U. J. INT'L L. & POL. 325, 326 (2015); Weill, *supra* note 8, at 180–81.

185. Kazmir, *supra* note 184, at 326. The New York Times conducted a 2014 study demonstrating the growth in terrorist ransom payments. Rukmini Callimachi, *Paying Ransoms, Europe Bankrolls Qaeda Terror*, N.Y. TIMES (July 29, 2014), http://www.nytimes.com/2014/07/30/world/africa/ransoming-citizens-europe-becomes-al-qaedas-patron.html?_r=0. In 2003, Al Qaeda was ransoming hostages at an average of $200,000 per hostage. *Id.* Compare this with 2008 where two Canadian hostages were ransomed for $1 million, and with 2013 where four French hostages were ransomed for $40 million. *Id.* The New York Times study concluded that between 2008 and 2015 Al Qaeda, and its supporting organizations, have made approximately $125 million through hostage negotiations and ransom payments. *Id.*

186. Kazmir, *supra* note 184, at 327. In 2014, ISIL had been paid approximately $20 million in ransom payments by various countries. David S. Cohen, Under Sec'y of the Treasury for Terrorism and Fin. Intelligence, Remarks at the Carnegie Endowment for International Peace: Attacking ISIL's Financial Foundation (Oct. 23, 2014).

A. *The Heightened Interest of International Terrorism*

When it comes to making ransom payments to terrorist organizations, there seems to be a heightened interest at play compared to paying ransoms to other brands of criminal organizations.[187] This could be due to the intense hostility toward terrorism and the heightened threat communities tend to perceive when confronted with terrorism.[188] In recent years, questions surrounding the wisdom of paying ransoms to terrorists have been thrust to the forefront of public attention, given the rise of ISIL.[189] ISIL is known to have taken hostages from at least twelve different countries, including the United States, England, Italy, Russia, France, Denmark, Sweden, Switzerland, Spain, and Belgium.[190] Many of these hostages have been ransomed and returned to their respective countries, while others are still being held by the organization.[191] The threat posed by international terrorism has led to it generally being treated as a heightened interest in terms of ransom and other laws.[192] The heightened interest is utilized as a policy argument in support of an outright ban on ransom payments to terrorist organizations, whereas, in other criminal enterprises, an outright ban on cooperative efforts is typically shied away from.[193]

Countries have taken different approaches to the problem of negotiating with and paying ransoms to terrorist organizations.[194] This patchwork of differing laws and policies is complicated further by international legal entities, such as the United Nations ("U.N."), which also has set forth extensive resolutions on the issue.[195]

187. Weill, *supra* note 8, at 184–85.

188. *Id.*

189. Kazmir, *supra* note 184, at 327.

190. *See* OFFICE OF THE HIGH COMM'R FOR HUMAN RIGHTS & U.N. ASSISTANCE MISSION FOR IR., REPORT ON THE PROTECTION OF CIVILIANS IN ARMED CONFLICT IN IRAQ: 6 JULY–10 SEPTEMBER 2014 3 (2014); Jethro Mullen, *How Many More Western Captives is ISIS Holding?*, CNN, http://www.cnn.com/2014/09/15/world/meast/isis-western-captives/ (last updated Sept. 15, 2014); Karen Yourish, *The Fates of 23 ISIS Hostages in Syria*, N.Y. TIMES (Feb. 10, 2015), http://www.nytimes.com/interactive/2014/10/24/world/middleeast/the-fate-of-23-hostages-in-syria.html?_r=0.

191. *See* Mullen, *supra* note 190; Yourish, *supra* note 190.

192. Bento, *supra* note 1, at 301–04; Dutton & Bellish, *supra* note 118, at 319–20.

193. Bento, *supra* note 1, at 301–04; Dutton & Bellish, *supra* note 118, at 319–20.

194. *See* Kazmir, *supra* note 184, at 328, 337–40.

195. *See id.* at 329.

B. *The International Law of Paying Ransoms to Terrorists*

The U.N. and other international legal entities have taken the broad, outward position that ransom payments should generally be banned.[196] However, this position, along with the resolutions passed by U.N. member-states, are not binding under international law.[197] In 2009, the U.N. passed Security Council Resolution 1904, which mandates that U.N. member-states freeze funds and assets in order to prevent ransom payments, but the resolution did not explicitly ban paying ransoms to terrorists.[198] Security Council Resolution 2133, which was passed in 2014, required states to prohibit terrorist organizations from "benefiting directly or indirectly from ransom payments."[199] Finally, in 2015, the U.N. passed Security Council Resolution 2199, which prohibits member-states from paying ransoms to terrorist organizations.[200] Security Council Resolution 2199 is surprisingly broad in its scope, in that the resolution prohibits the payment of any ransom payment by anyone, "regardless of how or by whom the ransom is paid," to a terrorist organization listed on a designated list of sanctioned terrorist organizations.[201] Despite the seemingly clear stance the U.N. has taken in its approach to paying ransoms to terrorists, its resolutions have not resulted in any prosecutions of either state-members or private individuals who have made ransom payments to prohibited terrorist organizations.[202]

The laws and policies supported by individual countries regarding ransom payments are far more complicated than the U.N.'s approach and send an inconsistent international approach to ransom payments.[203] Some countries, including the United States and the U.K. strongly oppose the practice of paying ransoms to terrorists.[204] On the other hand, there are countries, including Germany and France, which publicly take a stance against paying terrorist ransom demands, but have allegedly made such payments.[205]

---

196. *Id.* at 329–30.

197. *Id.* at 329.

198. S.C. Res. 1904, ¶ 1(a) (Dec. 17, 2009); *The Threat Posed by Kidnapping for Ransom by Terrorists and the Preventive Steps the International Community Can Take*, GOV.UK (June 18, 2013), http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207542/Kidnapping-for-ransom.pdf.

199. S.C. Res. 2133, ¶ 3 (Jan. 27, 2014).

200. S.C. Res. 2199, ¶ 19 (Feb. 12, 2015).

201. *Id.*

202. Kazmir, *supra* note 184, at 337.

203. *Id.*

204. *Id.* at 337–38.

205. *Id.* at 338; Yourish, *supra* note 190. France has actually made it illegal to provide financial, or other support, to terrorist organizations and it is unclear if French citizens

C. *The U.S. Approach to Paying Ransoms to Terrorists*

The United States takes the approach of banning ransom payments to terrorists and has tried to dissuade individual citizens from making such payments.[206] Families of U.S. hostages have accused the U.S. government of threatening them with legal prosecution if the families attempted to pay terrorists' ransom demands to secure the return of their family members.[207] In response to such accusations, the U.S. government has stated that it does not engage in threatening the families of hostages being held by terrorist groups, but claims it has a policy of informing such families of the laws in place that prevent the government or private U.S. citizens from making ransom payments to terrorist groups.[208] This dissuasion has led to some controversy between the U.S. government and U.S. citizens who want the government to support the release of their family members being held hostage.[209]

The Patriot Act is the legal instrument through which paying ransoms to terrorist organizations may be deemed illegal in the United States.[210] Section 2339B of the Patriot Act makes it unlawful for any person to knowingly provide material support to terrorist organizations.[211] This section imposes a prison sentence of between fifteen years to life for

---

would be prosecuted for paying terrorists' ransom demands in order to secure the release of their hostage family members. CODE PÉNAL [C. PÉN.] [PENAL CODE] art. 421-2-2 (Fr.).

206. Kazmir, *supra* note 184, at 338–39; Brian Ross et al., *'So Little Compassion': James Foley's Parents Say Officials Threatened Family Over Ransom*, ABC NEWS (Sept. 12, 2014, 5:58 PM), http://www.abcnews.go.com/International/government-threatened-foley-family-ransom-payments-mother-slain/story?id=25453963.

207. Michael Isikoff, *Sotloff's Parents Told They Could Be Prosecuted for Paying Ransom to IS*, YAHOO NEWS (Sept. 12, 2014), http://www.yahoo.com/news/sotloff-s-parents-were-told-they-could-be-prosecuted-for-paying-ransom-to-is-234329991.html?ref=gs; Paula Mejia, *U.S. Threatened James Foley's Family Over ISIS Ransom Demand, His Mother Says*, NEWSWEEK (Sept. 12, 2014, 5:16 PM), http://www.newsweek.com/us-threatened-james-foleys-family-over-isis-ransom-demand-270151. The families of two U.S. citizens, James Foley and Steven Sotloff, held hostage by ISIL, both reported being threatened with criminal prosecution by the U.S. government if they attempted to pay ISIL's ransom demands in exchange for their family members. Isikoff, *supra*; Mejia, *supra*.

208. Kazmir, *supra* note 184, at 339–40; Mejia, *supra* note 207.

209. *Family Releases Statement on Death of Warren Weinstein in U.S. Operation*, WASH. POST (Apr. 23, 2015), http://www.washingtonpost.com/news/post-nation/wp/2015/04/23/family-releases-statement-on-death-of-warren-weinstein-in-u-s-operation/?utm_term=.7a897b402cf9. Warren Weinstein was a U.S. citizen taken hostage by al-Qaeda. *Id.* Weinstein was killed by a drone strike conducted by the United States, while Weinstein was being held by the terrorist group. *Id.* Weinstein's wife would later express her desire for a more consistent approach by the U.S. government in aiding hostages and supporting their families. *Id.*

210. 18 U.S.C. § 2339B (2012).

211. *Id.* § 2339B(a)(1).

violations, depending on whether any loss of life results from the violation.[212] To violate section 2339B of the Act, the person providing material support must do so knowing that he or she is providing support to a terrorist organization.[213] Further, the violator must provide material support, which can be monetary support, training, advice, etc.[214] While there is nothing illegal under this section with the U.S. government or a private citizen having a conversation, or even negotiating with a terrorist organization, providing support—such as through a ransom payment—would violate this section of the Patriot Act.[215] However, section 2339C of the Patriot Act prohibits financing terrorism, attempting to finance terrorism, or conspiring to finance terrorism.[216] Thus, under section 2339C, the U.S. government or the family of a hostage may violate the Patriot Act by negotiating with terrorists under the Attempts and Conspiracy provisions of section 2339C.[217] This section, however, does include a heightened intent requirement, mandating that a violator of the section must intend that his or her support be used for terrorist activities.[218] If negotiations are permitted by section 2339C, the payment of ransoms to terrorist organizations would be a violation of both sections 2339B and 2339C.[219]

D. *Insurance Policies Covering Ransom Payments to Terrorists*

To offset the high prices of negotiation and ransom payments, some insurance companies offer kidnapping and ransom ("K&R") insurance.[220] These policies can cover a number of aspects in ransom negotiations, including fees necessary for consultations, any money lost while actually recovering the hostage, and the ransom payment itself.[221] While it is unclear how various countries will treat K&R insurance policies that seemingly flout

212. *Id.*

213. *Id.* However, in order for a violation to occur, it is not necessary that the person providing support knowingly further the terrorist activities of the terrorist organization. Holder v. Humanitarian Law Project, 561 U.S. 1, 16 (2010); United States v. Al Kassar, 660 F.3d 108, 129–30 (2d Cir. 2011). All that is necessary to violate the provision is that the person providing the support knew that their support was being given to a terrorist organization. *Holder*, 561 U.S. at 16–17.

214. 18 U.S.C. § 2339B(a)(1), (g)(4).

215. *Id.* § 2339B(a)(1); Kazmir, *supra* note 184, at 346.

216. 18 U.S.C. § 2339C(a)(2).

217. *Id.*; Kazmir, *supra* note 184, at 347.

218. 18 U.S.C. § 2339C(a)(1).

219. *Id.* § 2339B–C.

220. Meadow Clendenin, *"No Concessions" with No Teeth: How Kidnap and Ransom Insurers and Insureds Are Undermining U.S. Counterterrorism Policy*, 56 EMORY L.J. 741, 750 (2006).

221. *Id.* at 751–52.

laws by illegally providing financial support to terrorists, such as the Patriot Act, the U.K. has designed legislation intended to criminalize such policies.[222]

E. *Solutions to the Ransom Problem: The Terrorism Context*

The United States' rationale for banning ransom payments to terrorists is that doing so would place U.S. citizens at an even higher risk of being targeted as hostages by terrorist organizations.[223] The idea behind the argument in favor of an outright ban on paying ransoms to terrorists is that making such payments would only incentivize and legitimize the practice of hostage-taking and indirectly fund the terrorists' operations.[224] The downside to this argument is that placing a blanket ban on ransom payments reduces a ransom negotiator's flexibility to employ that option, which tends to result, as we often see, in a state actor or international entity paying the ransom anyway in direct violation of its own policy.[225] Closing the door entirely on negotiations cuts off any possibility of engaging in conversations that may prove beneficial from a *cost-benefit* perspective for the ransom negotiator.[226]

An approach that attempts to remedy this issue is referred to as a *process-structural approach*.[227] This approach is designed to "take the specific individual into consideration, while bolstering his or her bargaining power and reducing terrorists' incentives to kidnap."[228] First, this approach to dealing with terrorists' ransom demands is to be set out by statute to ensure the public understands their government's approach to dealing with the issue.[229] Next, any decision to accept or decline a ransom demand must be met with the approval of the Executive Branch and a majority of the Legislative Branch.[230] Deliberations over whether or not to accept the demand are to be conducted in private and the government will simply

222. Kazmir, *supra* note 184, at 357; *see also* 18 U.S.C. §§ 2339B–C; Sarah Veysey, *U.K. Terrorism Bill Proposes Ban on Insurance Coverage of Ransom Payments*, BUS. INS. (Dec. 7, 2014, 12:00 AM), http://www.businessinsurance.com/article/20141207/NEWS07/141209865?tags.

223. *Press Briefing by the Press Secretary, 11/18/2014*, WHITE HOUSE (Nov. 18, 2014, 1:00 PM), http://www.whitehouse.gov/the-press-office/2014/11/18/press-briefing-press-secretary-11182014.

224. Weill, *supra* note 8, at 192, 196.

225. *See id.* at 202–05.

226. *Id.* at 205.

227. *See id.* at 217.

228. *Id.*

229. Weill, *supra* note 8, at 211, 217.

230. *Id.* at 218. The theory is designed to aid democratic governments in addressing the issue of ransom demands by terrorists. *Id.*

answer whether they accept or decline the ransom demand.[231] The families of the hostages are to be given a hearing on the matter, during which the families can make their own case for paying or not paying the ransom.[232] The goal of this approach is to maximize a government's bargaining power by conducting closed-door discussions over whether the ransom deal would be to the country's advantage, while at the same time giving the entire ransom negotiation process uniformity, structure, and fairness to the hostages and their families.[233] Such a policy may give ransom negotiators enough flexibility to maximize the return for their party's interests, minimize their costs, and save lives.[234]

V. NEGOTIATING WITH RANSOMWARE HACKERS

Although never having to engage with a ransomware hacker is the best-case scenario, many healthcare organizations find themselves having to do so following a successful attack.[235] Ransom negotiators working on behalf of healthcare organizations in the face of a ransomware attack must deal with the same principles as ransom negotiators in other contexts: Maximizing benefits while minimizing costs, accounting for victim-based factors, and remaining in compliance with existing legal boundaries.[236]

A. *The Existing Legal Framework for Ransomware Negotiations: The Health Insurance Portability and Accountability Act ("HIPAA")*

HIPAA has become synonymous with private patient healthcare information.[237] HIPAA is intertwined with the threat posed by ransomware because the virus may steal electronic private patient information from healthcare providers.[238] A ransomware attack may rise to the level of a breach under HIPAA if the hacker actually obtains the protected patient

231. *Id.* at 220.
232. *Id.* at 225.
233. *See* Weill, *supra* note 8, at 220, 225, 230.
234. *See id.* at 217.
235. *See* CCIPS WHITE PAPER, *supra* note 12, at 2, 7.
236. *Id.* at 5, 7; Weill, *supra* note 8, at 217, 225.
237. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 1, 3 (2016).
238. *See* CCIPS WHITE PAPER, *supra* note 12, at 2; Zimmerman, *supra* note 5, at 16.

information, which would be an unpermitted disclosure "which compromises the security or privacy of the protected [personal] health information."[239]

1. Who Is Covered by HIPAA?

As a starting point, HIPAA only governs "covered entities and business associates."[240] Covered entities include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that transmit electronic information.[241] Covered entities also include health insurance companies, HMOs, employment-based health plans, Medicare, Medicaid, other government health insurance programs, and healthcare clearinghouses.[242] These covered entities must abide by HIPAA's numerous provisions and they may also be held liable under certain HIPAA provisions.[243]

2. The HIPAA Privacy Rule

The HIPAA Privacy Rule creates national standards designed to protect private health information.[244] The Privacy Rule applies to a certain type of information, known as *protected health information*.[245] Protected health information, also referred to as *individually identifiable health information*, is information relating to: "[T]he individual's past, present, or future physical or mental health or condition; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to the individual," which either identifies the specific person or which can reasonably identify that person.[246]

Individually identifiable health information cannot be used by covered entities for any reason other than reasons allowed in the Privacy Rule or if the individual, whose information is at issue authorizes, in writing, the information to be used for specific purposes.[247] The information cannot

239. 45 C.F.R. § 164.402 (2015); *see also* CCIPS WHITE PAPER, *supra* note 12, at 2; Zimmerman, *supra* note 5, at 16.

240. *Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited May 2, 2017).

241. *Id.*

242. *Id.*

243. *Id.*

244. U.S. DEP'T HEALTH & HUMAN SERVS., OCR PRIVACY BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003).

245. *Id.*

246. *Id.* at 3–4; *see also* 45 C.F.R. § 160.103 (2005).

247. U.S. DEP'T HEALTH & HUMAN. SERVS., *supra* note 244, at 4.

be disclosed by covered entities unless it is disclosed to the actual individuals, upon request, or to certain government agencies if there is an ongoing investigation.[248] Covered entities also may use or disclose this information for the organization to treat, pay, and conduct other healthcare activities.[249] Treatment includes "the provision, coordination, or management of healthcare and related services for an individual by one or more healthcare providers, including consultation between providers regarding a patient and referral of a patient by one provider to another."[250] Payment includes

> activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for healthcare delivered to an individual and activities of a healthcare provider to obtain payment or be reimbursed for the provision of healthcare to an individual.[251]

Healthcare operations include several actions, such as:

> (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: [D]e-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[252]

Further, the Privacy Rule requires covered entities to implement safeguards designed to ensure individually identifiable health information

248. 45 C.F.R. § 164.502(a)(2) (2005); U.S. DEP'T HEALTH & HUMAN. SERVS., *supra* note 244, at 4.

249. 45 C.F.R. § 164.506(c)(1)(i)–(ii) (2005); U.S. DEP'T HEALTH & HUMAN. SERVS., *supra* note 244, at 4–5.

250. U.S. DEP'T HEALTH & HUMAN. SERVS., *supra* note 244, at 5; *see also* 45 C.F.R. § 164.501 (2005).

251. U.S. DEP'T HEALTH & HUMAN. SERVS., *supra* note 244, at 5; *see also* 45 C.F.R. § 164.501.

252. U.S. DEP'T HEALTH & HUMAN. SERVS., *supra* note 244, at 5; *see also* 45 C.F.R. § 164.501.

remains private and is not made public intentionally or unintentionally.[253] Individuals also can request that covered entities restrict access to their individually identifiable health information strictly for the purposes of treatment, payment, and other healthcare activities.[254]

If a covered entity fails to abide by HIPAA's Privacy Rule, it may be subject to civil monetary penalties.[255] Penalties can range from $100 to over $50,000, with an annual cap on the amount an organization may be penalized of $1,500,000.[256] The penalty imposed depends on the circumstances of the privacy breach, including any possible intent or negligence on the part of the covered entity in regard to the privacy breach.[257] If the organization was not willfully negligent in regard to the privacy breach and the organization remedied the breach within thirty days of the organization discovering the breach or within thirty days of the day the organization should have known of the breach, then a civil penalty will not be imposed.[258] Criminal penalties also may be imposed for intentional breaches of the HIPAA Privacy Rule, which ranges depending upon the circumstances of the breach, with more egregious violations, such as violations committed with commercial motives, often resulting in penalties.[259]

3. The HIPAA Security Rule

The HIPAA Security Rule mandates that entities covered by the Act implement measures that can work to lower an entity's risk of any cyberattack.[260] The Security Rule applies to a specific type of protected health information, referred to as "electronic protected health information."[261] Electronic protected health information is protected health information transmitted by the organization using some electronic means.[262]

The Security Rule requires organizations to conduct regular risk analyses to detect potential vulnerabilities to the electronic protected health

253. 45 C.F.R. § 164.530(c)(1) (2005); U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 244, at 1, 3.

254. 45 C.F.R. § 164.522(a)(1) (2005); U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 244, at 4.

255. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 244, at 17.

256. *Id.* at 17–18.

257. *See id.*

258. *Id.* at 17.

259. *Id.* at 18.

260. *Summary of the HIPAA Security Rule*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (last visited May 2, 2017).

261. *Id.*

262. *Id.*

information being stored by the organization.[263] The organization then must work to minimize these vulnerabilities.[264] Organizations must have protocol in place to detect and prevent malicious software from infecting their computer systems.[265] Users of healthcare organization computer systems must be trained on how to protect their systems against malicious software, as well as reporting any suspicions that malicious software has infected one of the organization's systems.[266] The Security Rule also requires healthcare organizations to use access controls, allowing only necessary users to have access to electronic protected health information.[267] The Security Rule requires organizations to conduct a risk analysis of all threats to any electronic protected health information generated by the organization or its affiliates to determine if any electronic protected health information is in jeopardy of theft, exposure, or loss.[268] Covered entities must also ensure that their entire workforce is in compliance with the Security Rule.[269]

Although the Security Rule is somewhat similar to the Privacy Rule, in its application to electronic protected health information, the Security Rule does require two additional broad measures regarding health information.[270] First, organizations must maintain the integrity of electronic private health information under the Security Rule.[271] *Integrity* is defined by the Security Rule as ensuring that the electronic protected health information is not destroyed or altered without authorization.[272] The Security Rule also requires organizations to maintain electronic protected health information's availability.[273] *Availability* is defined by the Security Rule as maintaining the accessibility and usability of electronic protected health information.[274]

The Security Rule further requires covered entities to conduct a risk analysis, which must include several components.[275] The analysis must identify possible threats to electronic protected health information and assess

263. *Id.*
264. 45 C.F.R. § 164.306(a)(2) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.
265. *See* 45 C.F.R. § 164.306(a)(2), (e); *Summary of the HIPAA Security Rule*, *supra* note 260.
266. *See Summary of the HIPAA Security Rule*, *supra* note 260.
267. *Id.*
268. 45 C.F.R. § 164.306(a); *Summary of the HIPAA Security Rule*, *supra* note 260.
269. *Summary of the HIPAA Security Rule*, *supra* note 260.
270. *Id.*
271. 45 C.F.R. § 164.304 (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.
272. *Summary of the HIPAA Security Rule*, *supra* note 260.
273. *Id.*
274. *Id.*; 45 C.F.R. § 164.304.
275. *Summary of the HIPAA Security Rule*, *supra* note 260.

the impact of such threats, as well as the likelihood that they will occur.[276] The organization must develop measures to deal with the risks identified.[277] The measures taken to deal with security threats must be recorded.[278] Finally, the organization must maintain the security measures implemented.[279]

In order to ensure that these provisions are applied and upheld, healthcare organizations are required to name a security official whose role is to ensure that their organization is following through on these procedures.[280] Covered organizations are required to implement policies authorizing only certain staff members to have access to electronic protected health information.[281] Organizations must train and supervise all personnel handling electronic protected health information.[282] If a member of an organization's staff violates the organization's internal safeguards, the organization must issue appropriate sanctions.[283] Organizations must periodically review their procedures and ensure their staff is in compliance.[284]

The Security Rule also provides for a number of provisions designed to ensure the physical safety of electronic protected health information.[285] Organizations must ensure their physical facilities, where they keep the equipment storing their electronic protected health information, are secure.[286] Covered entities must also ensure that only authorized personnel are able to

276. 45 C.F.R. § 164.306(b)(2)(iv) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

277. 45 C.F.R. § 164.308(a)(1)(ii)(B) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

278. 45 C.F.R. §§ 164.306(d)(3)(ii)(B)(*1*), 164.316(b)(1) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

279. 45 C.F.R. § 164.306(e); *Summary of the HIPAA Security Rule*, *supra* note 260.

280. 45 C.F.R. § 164.308(a)(2) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

281. 45 C.F.R. § 164.308(a)(4)(i); *Summary of the HIPAA Security Rule*, *supra* note 260.

282. 45 C.F.R. § 164.308(a)(5)(i); *Summary of the HIPAA Security Rule*, *supra* note 260.

283. 45 C.F.R. § 164.308(a)(1)(ii)(C); *Summary of the HIPAA Security Rule*, *supra* note 260.

284. 45 C.F.R. § 164.308(a)(8); *Summary of the HIPAA Security Rule*, *supra* note 260.

285. 45 C.F.R. § 164.310(a)–(d) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

286. 45 C.F.R. § 164.310(a); *Summary of the HIPAA Security Rule*, *supra* note 260.

access devices storing electronic protected health information.[287] Further, the entity must have policies in place designed to protect its electronic protected health information during its "transfer, removal, disposal, and re-use."[288]

The HIPAA Security Rule imposes a number of technical safety measures, including access controls, which allow only certain users to access systems containing electronic protected health information and only for certain purposes.[289] Organizations also must install hardware, software, or other methods designed to record how the information is being used and accessed by the organization.[290] Steps must be taken to ensure that the information is not destroyed or modified without authorization, as well as steps taken to ensure the information is monitored to ensure it is not destroyed or modified.[291] Finally, the Security Rule requires organizations to take steps to ensure that electronic protected health information is secured and protected when being transmitted electronically.[292]

4. The HIPAA Breach Notification Rule

As an additional incentive to avoid putting electronic protected health information at risk, and to put those negatively affected on alert, HIPAA provides for a number of rules requiring healthcare organizations to notify different parties in the case of a breach.[293] These provisions make up HIPAA's Breach Notification Rule.[294] The Breach Notification Rule applies to all protected health information, not only electronic protected health information.[295] Under title 45, section 164.402 of the Code of Federal Regulations, a breach is defined as: "[T]he acquisition, access, use, or disclosure of protected health information in a manner not permitted, . . . which compromises the security or privacy of the protected health information."[296] Any impermissible use of protected health information is

287. 45 C.F.R. § 164.310(b)–(c); *Summary of the HIPAA Security Rule*, *supra* note 260.

288. *Summary of the HIPAA Security Rule*, *supra* note 260; *see also* 45 C.F.R. § 164.310(d)(i)–(iv).

289. 45 C.F.R. § 164.312(a)–(e) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

290. 45 C.F.R. § 164.312(b); *Summary of the HIPAA Security Rule*, *supra* note 260.

291. 45 C.F.R. § 164.312(c); *Summary of the HIPAA Security Rule*, *supra* note 260.

292. *Summary of the HIPAA Security Rule*, *supra* note 260.

293. *See* 45 C.F.R. §§ 164.400–.414 (2015).

294. *Id.*; *Breach Notification Rule*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/breach-notification/ (last visited May 2, 2017).

295. *See* 45 C.F.R. § 164.400.

296. 45 C.F.R. § 164.402.

presumptively a breach requiring notification, unless the covered entity is able to demonstrate that there is a low likelihood the protected health information was actually compromised based on several factors.[297] Not included as a breach under the rule are:

> (i) [a]ny unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted [by the rule]; (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted [by the rule]; [and] (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.[298]

If a covered entity commits a breach that involves unsecured protected health information, the entity is required to make disclosures to the U.S. Department of Health and Human Services, any individuals who may be affected by the breach, and, depending on the circumstances, to the public through the media.[299] Unsecured protected health information is defined as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology [as] specified" by the Department of Health and Human

---

297. *Breach Notification Rule*, *supra* note 294; *see also* 45 C.F.R. § 164.402(2).

> (1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) [t]he unauthorized person who used the protected health information or to whom the disclosure was made; (3) [w]hether the protected health information was actually acquired or viewed; and (4) [t]he extent to which the risk to the protected health information has been mitigated.

45 C.F.R. § 164.402(2)(i)–(iv).

298. 45 C.F.R. § 164.402(1)(i)–(iii).

299. *Breach Notification Rule*, *supra* note 294; *see also* 45 C.F.R. § 164.406(a) (2015).

Services.[300] Covered entities must only disclose to the media if over 5002 residents of a certain jurisdiction are affected by an entity's breach.[301]

B. *Best Practices for Healthcare Organizations to Avoid Ransomware Attacks*

Of course, never ending up in a situation where one has to negotiate with a ransomware hacker is the most effective means of protecting a healthcare organization's information and resources.[302] The U.S. government has encouraged that systems administrators and computer users take certain preventive steps to lower the risk of a successful ransomware attack.[303]

1. Backup—and Then Backup Your Backup

Backing up all electronic data to a secured backup location can prevent a terrible situation from becoming a nightmare.[304] A healthcare organization with a secured, isolated backup at an isolated location can restore its computer system in approximately four hours.[305] These backups should be tested and assessed annually to ensure they can deal specifically with a ransomware threat.[306] Once a computer is infected with ransomware, the virus can move between computers using the same network, which is why it is imperative to store backup data outside of the original network to ensure it also would not be exposed to the virus.[307] External backups can be stored in a cloud-based system or stored in physical form.[308]

300. 45 C.F.R. § 164.402(2)(iv).
301. 45 C.F.R. § 164.406(a).
302. *See* CCIPS WHITE PAPER, *supra* note 12, at 3, 5.
303. *Id.* at 3–4.
304. *See 10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
305. *Id.*
306. CCIPS WHITE PAPER, *supra* note 12, at 4.
307. DUNBRACK, *supra* note 19, at 2; CCIPS WHITE PAPER, *supra* note 12, at 4.
308. CCIPS WHITE PAPER, *supra* note 12, at 4. Although, there are variants of the ransomware virus that are capable of infecting backups located on cloud-based storage systems if those systems regularly back up the original system automatically. *Id.* at 6. This method of automatic back up from a cloud-based system is referred to as *persistent synchronization*. *Id.* at 4. Healthcare organizations with a persistent synchronization back up network may want to consider utilizing a separate back up network as well. *See id.*

2. Controlling Access to Operating Systems

Perhaps not every healthcare organization staff member requires access to the organization's shared network to perform their tasks and, therefore, access to the network can be limited based on priority.[309] Administrative access to shared networks should only be granted if necessary and limiting the use of access can reduce the window of opportunity that a ransomware hacker has to infiltrate the network.[310] Access controls can also be used to limit the files a user is able to access, thus controlling the potential danger zones a user can access.[311]

3. Monitoring Inbound and Outbound Emails

Although newer versions of the ransomware virus no longer require an employee to open a dangerous email, the older virus is still being used and other viruses are also dispatched in this manner.[312] Known as *phishing emails*, these treacherous emails only pose a threat if they are opened by an employee.[313] While training and awareness programs can be effective at reducing the risk of an employee opening these false emails, some hackers are very skilled at making the emails appear authentic and important.[314] Along with a prevention training program, healthcare organizations should take efforts to ensure these emails never reach their employees in the first place.[315] Spam filters can be enabled to detect these malicious emails, and authentication technologies are available to detect emails being sent from unknown locations.[316] System administrators should also monitor inbound and outbound emails for suspicious activity.[317]

---

309. *Id.*

310. CCIPS WHITE PAPER, *supra* note 12, at 3–4.

311. *Id.* at 4.

312. *Id.* at 3.

313. *Id.*; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

314. *See* CCIPS WHITE PAPER, *supra* note 12, at 3. Hackers have used a virus variant that sends an authentic-appearing email to an employee, listing that employee's employer as the sender. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5. The unsuspecting employee is more likely to open an urgent, yet spam, email from their boss than they are to open an email from an anonymous or unfamiliar sender. *Id.*

315. CCIPS WHITE PAPER, *supra* note 12, at 3.

316. *Id.* Among these different verification programs are "Sender Policy Framework ("SPF"), Domain Message Authentication Reporting and Conformance ("DMARC"), and DomainKeys Identified Mail ("DKIM")." *Id.*

317. *Id.*

4. Human Error Is the Greatest Risk

Although not all versions of the ransomware virus depend on human action, many versions infect computers by deceiving computer users into clicking links or opening emails.[318] One of the simplest preventive steps a healthcare organization can take to defend itself from ransomware attacks is to inform its personnel of the risk posed by ransomware, common methods by which the virus is used to infect computers; and actions to avoid while using a healthcare server, such as clicking on advertisements, browsing unnecessary websites, or opening emails that seem in any way suspicious.[319] A training and awareness program specific to the threat of ransomware, along with periodic reminders, can go a long way toward preventing an attack.[320]

5. Cyber-Defensive Measures

As mentioned previously, some variants of ransomware are able to breach an organization's shared network due to vulnerabilities or unpatched areas in the system's network.[321] The risk of this type of ransomware variant being successful can be mitigated by employing a *patch management system* to detect and prevent holes in the system's network.[322] Other more common methods of defending computer systems include setting up firewalls that block unknown IP addresses and ensuring anti-virus and anti-malware settings are set to scan for threats.[323]

6. How HIPAA Helps

If complied with, HIPAA's numerous provisions can aid a healthcare organization in protecting itself from ransomware and all other cyberattacks.[324] HIPAA's Security Rule requires organizations covered by the law to implement a risk assessment plan and to actively minimize the cybersecurity risks identified in the plan.[325] The Security Rule also requires covered organizations to train personnel with access to electronic protected health information and to designate a security official in charge of managing

318. DUNBRACK, *supra* note 19, at 2; CCIPS WHITE PAPER, *supra* note 12, at 3.
319. CCIPS WHITE PAPER, *supra* note 12, at 3.
320. *Id.*
321. DUNBRACK, *supra* note 19, at 2.
322. CCIPS WHITE PAPER, *supra* note 12, at 3.
323. *Id.*
324. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 244, at 4.
325. 45 C.F.R. § 164.306(a)(2) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

access to electronic protected health information.[326] Further, the Security Rule requires covered organizations to impose access controls regarding which employees may access this information.[327]

HIPAA's Enforcement Rule gives the law teeth by imposing disclosure requirements on organizations which experience certain types of breaches pertaining to their stored protected health information.[328] The Enforcement Rule requires healthcare organizations to disclose breaches of certain magnitudes to the individuals affected, the press, or the government.[329] These penalties encourage healthcare organizations to abide by HIPAA's Privacy and Security Rule provisions, which can minimize the risk of a ransomware attack in the first place.[330] These disclosure requirements will also help to inform individuals affected by a data breach to enable them to take steps to protect themselves.[331]

7. Dealing with a Ransomware Attack

If a computer or operating system is infected with the ransomware virus, the U.S. Government further suggests the organization take certain steps to deal with the attack.[332] If the virus is detected early enough that it has only infected one or a small number of computers, those computers should be disconnected from the organization's network to prevent the virus from spreading further.[333] If there are computers that have been infected, but not entirely disabled, these computers should also be disconnected from the network and shut down.[334] If the organization has a backup system, this should be monitored to ensure it has not been infected by the virus, and if the backup is connected to the same network as the original system, the backup should be disconnected from the network.[335] The U.S. Government also recommends that organizations contact the FBI or the Secret Service if they fall victim to a ransomware attack.[336] The organization should then secure as

326. *See* 45 C.F.R. § 164.306(e), .308(a)(2) (2015); *Summary of the HIPAA Security Rule*, *supra* note 260.

327. 45 C.F.R. § 164.306(a); *Summary of the HIPAA Security Rule*, *supra* note 260.

328. 45 C.F.R. § 164.402 (2015); *Breach Notification Rule*, *supra* note 294.

329. 45 C.F.R. § 164.402; *Breach Notification Rule*, *supra* note 294.

330. *See Breach Notification Rule*, *supra* note 294.

331. *See* 45 C.F.R. § 164.402; *Breach Notification Rule*, *supra* note 294.

332. CCIPS WHITE PAPER, *supra* note 12, at 4–5.

333. *Id.*; *see also* DUNBRACK, *supra* note 19, at 10.

334. CCIPS WHITE PAPER, *supra* note 12, at 4; *see also* DUNBRACK, *supra* note 19, at 10.

335. CCIPS WHITE PAPER, *supra* note 12, at 5; *see also* DUNBRACK, *supra* note 19, at 11; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

336. CCIPS WHITE PAPER, *supra* note 12, at 5.

much of its uninfected system as possible and change any passwords associated with the network, if possible.[337] Finally, the U.S. Government does not recommend paying ransoms to ransomware hackers.[338]

8. The Role of Law Enforcement

The U.S. Government recommends that organizations infected with ransomware make contact with law enforcement.[339] Law enforcement, such as the Secret Service or the FBI, may be able to tap into resources able to help the organization, to which the organization—acting alone—would not have access.[340] One such resource would be the international law enforcement community, which can aid in tracking down international hackers or foreign variants of the virus.[341] While notifying law enforcement may seem futile or embarrassing in ransomware cases, law enforcement officials have been successful in several ransomware cases.[342]

Despite these best practices, all organizations face a strong possibility of being attacked successfully by a ransomware hacker.[343] Healthcare organizations, along with each and every one of their users, must be vigilant at all times to prevent these attacks, whereas, a ransomware hacker only has to get lucky once.[344] This state of constant defense does not bode well for healthcare organizations with the result being that sooner or later many organizations will find themselves negotiating with ransomware hackers.[345]

C. *Negotiation Solutions to the Ransom Problem: The Ransomware Context*

If ransomware hackers are able to infect a healthcare organization's system with the virus, the organization is faced with two options: (1) pay the

337. *Id.*

338. *Id.*; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

339. CCIPS WHITE PAPER, *supra* note 12, at 5.

340. *Id.*

341. *Id.*

342. Zimmerman, *supra* note 5, at 16. For example, in mid-2014 the U.S. Department of Justice was able to takedown an entire malware system being used to launch ransomware attacks. *Id.* This system was known as Gameover ZeuS. *Id.*

343. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

344. Zimmerman, *supra* note 5, at 16; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

345. *See 10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

ransom or (2) do not pay the ransom.[346] Paying the ransom is the only realistic hope of having the virus removed from the system.[347] However, paying the ransom with the hope that the virus will be lifted rests on a number of assumptions.[348] First, if the virus depends on a decryption key to unlock the infected computer, the organization is assuming that if its pays, the hacker will give it the decryption key.[349] Second, the organization assumes that if it is given the decryption key, it will actually work and remove the virus.[350] Third, the organization assumes that if the decryption key is provided and effectively removes the virus, that the virus will be removed from all of its systems and not just some of its systems.[351] Fourth, the organization assumes that the ransomware hacker will not simply hack it again after seeing their efforts rewarded.[352] On the other hand, refusing to pay the ransom would result in practically zero chance of lifting the virus, which, when dealing with healthcare organizations, can result in lost time, resources, and patient information, all of which can be especially critical in the healthcare context.[353] However, this may be an acceptable loss if the proper protocols have been adhered to.[354]

As discussed in the context of piracy above, the various interests of the opposing parties in the ransomware context must also be considered and each outcome predicted when deciding whether or not to pay ransom demands.[355] The successfully hacked healthcare organization may either pay the ransom or refuse to pay the ransom.[356] The successful hacker may either release the hostage computer system, along with all of its data, or refuse to release the system, leaving it infected and unusable.[357] The only win-win situation here occurs where the healthcare organization pays the ransom and the ransomware hacker releases the computer system.[358] The healthcare organization will regain its ability to function and provide healthcare services

346. *Id.*
347. *Id.*
348. *Id.*
349. *Id.*
350. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
351. *Id.*
352. *Id.*
353. Zimmerman, *supra* note 5, at 16.
354. DUNBRACK, *supra* note 19, at 9–11; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
355. Bento, *supra* note 1, at 326, 330; *see also supra* Section III.E.
356. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
357. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.
358. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

and the ransomware hacker will have realized his or her financial goal.[359] A second resolution arises where the healthcare organization decides to pay the ransom demand, but the ransomware hacker refuses to release the computer system from the virus, despite the payment.[360] This resolution plays out fairly often, unfortunately, since ransomware hackers are not the most honest of criminals, making payment of ransom demands a less-than-appealing option.[361] This is a lose-win situation for the hospital and the hacker, respectively.[362] The next outcome, in which the healthcare organization decides not to pay the ransom demand and the ransomware hacker chooses to release the hostage computer system, is a win-lose outcome favoring the healthcare organization and will almost never occur because the ransomware hacker has already succeeded in attacking the organization's computer system and, therefore is in a superior bargaining position in which he or she unlikely would act contrary to his or her own interest.[363] The final outcome—in which the healthcare organization chooses not to pay the demanded ransom, and the hacker chooses not to release the hostage computer system—is a lose-lose scenario in which the organization will not recover its lost system functioning, and the hacker will not realize his or her financial goal.[364]

---

359. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

360. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

361. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5. This was the case where a ransomware hacker successfully infected a Kansas-based hospital with the ransomware virus. *Id.* The hospital chose to pay the ransom, likely hoping that the first outcome would occur where the hospital regains functioning of its computer systems and the hacker is satisfied with their reward. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; *see also* Bento, *supra* note 1, at 326, 330. However, instead of honoring their agreement, upon receiving the ransom sum, the hacker released only part of the hospital's operating system. *10-Minute Guide to Ransomware Protection*, *supra* note 5. The hacker then demanded further ransom payments to release the rest of the system—a significant portion of the system—from the ransomware virus. *Id.* Thus, while hoping to achieve the first outcome of the possible resolutions to a ransom negotiation, this negotiation ended up reaching the second outcome, in which the hospital pays the ransom and the ransomware hacker refuses to release the computer system from the virus. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Ransomware Protection*, *supra* note 5. This is a lose-win situation for the hospital and the hacker, respectively. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

362. Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

363. Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

364. *See* Bento, *supra* note 1, at 321, 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

Similar to the context of piracy, this outcome-based framework for analyzing ransomware negotiations is insufficient on its own for several reasons.[365] As in the piracy context, each option cannot be given equal weight because the outcome in which the healthcare organization does not pay the ransom, and the ransomware hacker releases the computer system will almost certainly not occur—the outcome in which the healthcare organization pays the ransom and the hacker does not release the parts of, or the entire computer system, is a possibility and has occurred in the past—and the situation where the healthcare organization pays the ransom, and the hacker releases the computer system, is actually not a win at all for the healthcare organization; in fact, it is a serious loss.[366] The healthcare organization will have lost resources for the amount used to pay the hacker for the downtime suffered during the negotiation and—worst of all—for any stolen protected patient information.[367] However, if the healthcare organization has adhered to the best practices for preventing a ransomware attack prior to being attacked, it will have backed up all of its electronic information onto a separate server, safe from the ransomware attack.[368] This action would mitigate the potential damage if the organization chooses not to pay the ransom and does not recover the system controlled by the hacker.[369] A system backup would further allow the organization to recommence operation much faster than would be possible if the organization engages in negotiations with the hacker.[370] This scenario makes the lose-lose outcome more appealing, especially considering that at any point after a ransomware hacker takes control of a computer system, a hacker could steal protected patient data.[371] Thus, under any of the four outcomes, protected patient data could be stolen, resulting in a significant loss for the healthcare organization and its patients.[372]

365. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; *supra* Section III.E.

366. *See* Bento, *supra* note 1, at 326, 330; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; *supra* Section III.E.

367. Beek, *supra* note 14.

368. DUNBRACK, *supra* note 19, at 11; Zimmerman, *supra* note 5, at 16; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

369. *See* DUNBRACK, *supra* note 19, at 11; Zimmerman, *supra* note 5, at 16; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

370. *See* DUNBRACK, *supra* note 19, at 11; Zimmerman, *supra* note 5, at 16; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5. In fact, if the organization engages with and pays a ransomware hacker, the organization may never regain control over its stolen computer system. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

371. *See* Zimmerman, *supra* note 5, at 16; Hagland, *supra* note 14.

372. *See* Zimmerman, *supra* note 5, at 16; Hagland, *supra* note 14.

1. Arguments in Favor of Paying Ransoms to Ransomware Hackers

The arguments in favor of paying ransoms to pirates and terrorists are similar to the arguments in favor of paying ransoms to ransomware hackers, including: The possibility of recovering the hostage data and the notion that ransom negotiators should not limit their options by removing the possibility of paying ransoms.[373] However, the digital nature of the hacker ransom demand transaction can allow hackers to back out on their side of the agreement with greater ease than a pirate, or terrorist, who takes people hostage.[374] Where both sides of a ransom negotiation are entirely digital, the possibility of recovering the hostage data decreases substantially.[375]

2. Arguments Opposed to Paying Ransoms to Ransomware Hackers

Once again, the arguments in the contexts of piracy and terrorism are similar to the arguments opposed to paying ransoms to ransomware hackers, including: The idea that ransom payments will only further the ransomware hacking enterprise; the argument that paying a ransomware ransom may expose the organization as vulnerable and willing to pay out, which encourages future ransomware attacks; and the argument that ransomware hackers may simply accept the ransom payment and sell off the ransomed data on the black market.[376] These arguments are compelling in greater part because they have been proven accurate based on ransomware attacks on healthcare organizations in the past.[377] However, imposing an outright ban on healthcare organizations paying ransom payments to ransomware hackers would unnecessarily deprive negotiators of a valuable option in the negotiation.[378] Further, there may be nothing to be gained by depriving healthcare organizations of the right to pay ransom to ransomware hackers because these hackers will have an incentive to use the virus and demand ransom, even if they are fully aware that healthcare organizations are banned from paying them.[379] The hackers still have an incentive to hack the

373. *See* Bento, *supra* note 1, at 326, 330; Dubner & Chavers, *supra* note 126, at 317–19, 327; Weill, *supra* note 8, at 200, 204–05.

374. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

375. *See* Bento, *supra* note 1, at 289; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

376. Bento, *supra* note 1, at 288–89; Dutton & Bellish, *supra* note 118, at 309–11; Weill, *supra* note 8, at 192, 194, 197; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

377. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

378. *See* Gifford, *supra* note 1, at 60–62; Reynolds, *supra* note 132, at 612; CCIPS WHITE PAPER, *supra* note 12, at 5.

379. Zimmerman, *supra* note 5, at 16; Hagland, *supra* note 14.

organizations to steal their valuable, protected patient data and they still may demand ransom payments, hoping that the organizations will pay regardless of the ban, perhaps in order to make the problem go away quietly.[380]

D. *Alternative Solutions to the Ransomware Problem*

Although an outright ban on ransom payments to ransomware hackers may be too restrictive of an option for negotiators, other alternative solutions can be employed to help combat the issue using the legal landscape.[381]

1. A Heightened Terrorist-esque Interest for Ransomware Negotiations

As mentioned above, the problem of terrorism has been accorded a heightened interest, which is used by many countries to justify an all-out ban on ransom payments to terrorists, as well as enabling several other practices considered too extreme to use in response to other crimes.[382] The idea behind this heightened interest is that terrorism is a uniquely difficult problem that cannot be solved using conventional methods alone.[383] Whether the threat posed by ransomware necessarily rises to the level where it would warrant an all-out ban on ransom payments need not be answered because of the unique electronic nature of the entire ransomware transaction, and the incentive of ransomware hackers to use the virus in order to steal protected patient data resulting in no beneficial purpose to be gained by an all-out ban on ransom payments.[384]

2. Imposing a Tax on Ransomware Payments to Be Used for Anti-Hacking Efforts

An alternative method of reducing the incentives of ransom negotiators to pay the ransom—and of hostage takers to take hostages to begin with—is to impose a tax on ransom payments made, with the proceeds being used to combat the ransomware problem.[385] This solution has been discussed in the context of piracy ransom negotiations.[386] In the ransomware

380. Zimmerman, *supra* note 5, at 16; Hagland, *supra* note 14.

381. *See* Gifford, *supra* note 1, at 60–62; Reynolds, *supra* note 132, at 612; CCIPS WHITE PAPER, *supra* note 12, at 5.

382. Weill, *supra* note 8, at 180–81.

383. *Id.* at 181.

384. *See* Gifford, *supra* note 1, at 60–62; Reynolds, *supra* note 132, at 612–13; CCIPS WHITE PAPER, *supra* note 12, at 5.

385. *See* Bento, *supra* note 1, at 332.

386. *Id.*

context, a federal tax could be imposed on all ransom payments made to ransomware hackers and the proceeds could be used to fund federal efforts to prevent cyberattacks.[387] Such a tax reduces the incentive of healthcare organizations to pay ransoms to ransomware hackers because doing so would result in them having to pay an additional sum on top of the ransom payment.[388] The tax also reduces the incentive of ransomware hackers to demand ransom from these organizations because doing so will indirectly fund government efforts aimed at preventing cyberattacks in the first place.[389] The major shortfall of this alternative approach is that healthcare organizations may become even less likely to report ransomware incidents to avoid the imposed tax.[390]

3. Prohibiting Insurance Coverage for Ransomware Attacks

Insurance companies have been offering coverage to companies and individuals facing ransom situations, such as K&R policies in the terrorism context.[391] Noting the rising threat of cyber-hacking in today's world, many different forms of cyber insurance are now available.[392] Cyber-insurance seeks to cover insured entities for the cost of digital loss and repair following a cyberattack on the insured's computer network.[393] Healthcare organizations have an incentive to purchase cyber insurance as coverage can aid an organization financially in recovering from a debilitating attack.[394]

387. *See id.* at 332–33.

388. *See id.* Reducing the incentive of healthcare organizations to pay ransoms to hackers, hoping to ensure that their lost network will be functioning, is an important goal considering how often healthcare organizations pay the ransom demand and the ransomware hackers refuse to restore the organization's network or make additional ransom demands. *See id.*; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5. Further, once a healthcare organization pays a ransom demand, it may be seen by other hackers as vulnerable, increasing the likelihood that they will be attacked again. *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

389. Bento, *supra* note 1, at 332.

390. *See* Bento, *supra* note 1, at 332; CCIPS WHITE PAPER, *supra* note 12, at 5; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

391. Clendenin, *supra* note 220, at 750.

392. *See* Jean Bolot & Marc Lelarge, *Cyber Insurance as an Incentive for Internet Security, in* MANAGING INFORMATION RISK AND THE ECONOMICS OF SECURITY 269, 273 (M. Eric Johnson ed., 2009); RUPERTO P. MAJUCA ET AL., THE EVOLUTION OF CYBERINSURANCE 2 (2006); Kathleen Richards, *Is Cyberinsurance Worth the Risk?*, TECHTARGET, http://searchsecurity.techtarget.com/feature/Is-cyberinsurance-worth-the-risk (last updated Aug. 2014).

393. *See* Bolot & Lelarge, *supra* note 392, at 270–71; MAJUCA ET AL., *supra* note 392, at 3; Richards, *supra* note 392.

394. *See* Bolot & Lelarge, *supra* note 392, at 270–71; MAJUCA ET AL., *supra* note 392, at 2–3; Richards, *supra* note 392.

However, many organizations choose not to purchase cyber-insurance because, among other reasons, the organizations do not want to disclose that its system has been compromised following an attack, because doing so may expose the organization as vulnerable to future attacks.[395]

Although some would argue that ransom-based insurance policies promote security, since the occurrence of successful cyberattacks are nearly inevitable, others argue that this type of coverage only lulls covered organizations into a false sense of security and results in the organization failing to implement other appropriate safeguards to prevent ransom situations from arising.[396] The major difference here between the ransomware context and the contexts of terrorism and piracy is that ransomware hackers may obtain something of value from healthcare organizations merely by taking the organization's system hostage: Protected patient information.[397] Unlike human hostage situations, where the criminals are only successful if their ransom demands are met, ransomware hackers are still successful even if their demands are not met.[398] Cyber-insurance can help a healthcare organization regain a functioning network in the face of an attack, but the organization still has every incentive to take other steps to protect its system because cyber-insurance typically does not help the organization with respect to HIPAA claims and other liability due to lost patient data.[399]

4. Requiring Healthcare Organizations to Pass Annual Cyber-Inspections and Employ Cyber-Guards

HIPAA already places several requirements on healthcare organizations pertaining to its electronic protected health information, including a requirement that the organization conduct regular risk analyses on its electronic security measures.[400] This requirement could be expanded to require healthcare organizations to pass an annual cyber-inspection every

395. *See* Richards, *supra* note 392.

396. *See* Bolot & Lelarge, *supra* note 392, at 277; MAJUCA ET AL., *supra* note 392, at 2–3; Clendenin, *supra* note 220, at 750–51; Richards, *supra* note 392.

397. *See* CCIPS WHITE PAPER, *supra* note 12, at 8; Zimmerman, *supra* note 5, at 16.

398. *See* Weill, *supra* note 8, at 205–07, 217; Zimmerman, *supra* note 5, at 16; CCIPS WHITE PAPER, *supra* note 12, at 8.

399. Bolot & Lelarge, *supra* note 392, at 270–71; MAJUCA ET AL., *supra* note 392, at 2–3; *Breach Notification Rule*, *supra* note 294; Richards, *supra* note 392; *Summary of HIPAA Security Rule*, *supra* note 260.

400. 45 C.F.R. § 164.306(a)(1) (2015); *see also Breach Notification Rule*, *supra* note 294; *Summary of HIPAA Security Rule*, *supra* note 260.

year by an authorized institution.[401] Such a requirement would push healthcare organizations to ensure its electronic protected health information is protected to clear inspection.[402]

Further, an alternative solution raised by some in the piracy context is to require ship-owners to employ guards on their vessels when they know their crew is being sent into pirate-infested waters.[403] This solution could be applied to the ransomware context by requiring healthcare organizations to employ electronic data protection experts to conduct regular performance reviews of a healthcare organization's security measures.[404]

5. A Process-Structural Approach to Ransomware Ransom Payment Decision-Making

An alternative solution proposed in the terrorism context, as opposed to an outright ban on ransom payments to terrorists, is what is described as a *process-structural approach*.[405] The process-structural approach to ransom payments requires a clear legal standard determining when, and how the decision to pay a ransom demand will be reached.[406] The approach requires a distinct group of decision-makers to reach a consensus privately as to whether or not they will agree to the ransom demand.[407] Finally, the human and personal factors involved are taken into account, with those who will be affected by the decision being given the opportunity to be heard by the decision-makers.[408] The process-structural approach is ideal in the terrorism or even the piracy context because it allows an existing decision-making body, a democratic government, to reach a contemplated consensus while promoting both transparency behind its approach, as well as a private means of reaching a decision.[409] Unfortunately, this approach would be inapplicable to the context of ransomware because the approach requires decision-makers to engage in a lengthy process of discussion in order to

401. *See* 45 C.F.R. § 164.306(b)(1); *Breach Notification Rule*, *supra* note 294; *Summary of HIPAA Security Rule*, *supra* note 260.

402. *See* 45 C.F.R. § 164.306(c); *Breach Notification Rule*, *supra* note 294; *Summary of HIPAA Security Rule*, *supra* note 260.

403. Bento, *supra* note 1, at 331–32.

404. *See* 45 C.F.R. § 164.308(a)(2) (2015); *Summary of HIPAA Security Rule*, *supra* note 260. HIPAA already requires covered organizations to designate an individual in charge of ensuring the organization complies with HIPAA-required safeguards pertaining to protected patient information. 45 C.F.R. § 164.308(a)(2); *Summary of HIPAA Security Rule*, *supra* note 260.

405. Weill, *supra* note 8, at 217–18.

406. *Id.* at 218.

407. *Id.* at 217.

408. *Id.* at 217–18.

409. *Id.*

reach a consensus, which cannot work in the face of a ransomware attack where a virus is employed that steals protected patient data over time.[410]

VI. CONCLUSION

The threat of ransomware likely will only increase as the virus is modified to overcome cyber-defenses in the healthcare industry, which seems to continually struggle to keep up with technological advancements.[411] Despite the persistence of ransomware hackers, understanding the preemptive steps healthcare organizations can take to protect their electronic-protected patient information and complying with HIPAA's other, numerous requirements will ideally protect healthcare organizations from many ransomware attacks.[412] If and when, however, these defenses fail and a hacker is successful at infecting a healthcare system with the ransomware virus, understanding the advantages and disadvantages of various negotiation-based approaches can help the organization manage the crisis as best as possible.[413] Further, there are ways that the legal landscape can be changed to better fight the ransomware problem.[414] Alternative methods such as taxing ransom payments, imposing stricter cyber testing requirements, and requiring inspections by experts in the cyber security field can be helpful legal tools to curb the ransomware problem without depriving negotiators of the option to pay the ransomware hacker's demands or, at least, allow the hacker to believe the organization may pay his or her demands.[415] These options demonstrate how different approaches, such as the negotiation theory approach, can be utilized to better understand and fight the growing ransomware menace.[416]

---

410. *See* Weill, *supra* note 8, at 217–18; CCIPS WHITE PAPER, *supra* note 12, at 2.

411. DUNBRACK, *supra* note 19, at 2; O'GORMAN & MCDONALD, *supra* note 10, at 10; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5.

412. U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 244, at 1; *see also* DUNBRACK, *supra* note 19, at 2; O'GORMAN & MCDONALD, *supra* note 10, at 10; *10-Minute Guide to Healthcare Ransomware Protection*, *supra* note 5; *Breach Notification Rule*, *supra* note 294; *Summary of the HIPAA Security Rule*, *supra* note 260.

413. *See* CRAVER, *supra* note 103, at 11–12; PUNNETT, *supra* note 103, at 412; Gifford, *supra* note 1, at 46.

414. *See* 45 C.F.R. § 164.306(a) (2015); Bento, *supra* note 1, at 332; *Breach Notification Rule*, *supra* note 294; *Summary of the HIPAA Security Rule*, *supra* note 260.

415. 45 C.F.R. § 164.306(a); Bento, *supra* note 1, at 332; *Breach Notification Rule*, *supra* note 294; *Summary of the HIPAA Security Rule*, *supra* note 260.

416. CRAVER, *supra* note 103, at 11–12; *see also* PUNNETT, *supra* note 103, at 412; Gifford, *supra* note 1, at 46.